MINISTÉRIO DA DEFESA

MD31-P-03

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA O SISTEMA MILITAR DE COMANDO E CONTROLE

2015

MINISTÉRIO DA DEFESA
ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA O SISTEMA MILITAR DE COMANDO E CONTROLE

2ª Edição
2015

MINISTÉRIO DA DEFESA
GABINETE DO MINISTRO

PORTARIA NORMATIVA Nº 2.327/MD, DE 28 DE OUTUBRO DE 2015.

Dispõe sobre a Política de Segurança da Informação para o Sistema Militar de Comando e Controle - MD31-P-03 (2ª Edição/2015).

O **MINISTRO DE ESTADO DA DEFESA**, no uso das atribuições que lhe conferem o art. 87, parágrafo único, inciso II, da Constituição Federal, o art. 27, inciso VII, alínea “b”, da Lei nº 10.683, de 28 de maio de 2003, e o art. 1º, inciso II, do Anexo I do Decreto nº 7.974, de 1º de abril de 2013, e tendo em vista o que consta do processo nº 60080.000784/2015-40, resolve:

Art. 1º Aprovar a Política de Segurança da Informação para o Sistema Militar de Comando e Controle - MD31-P-03 (2ª Edição/2015), na forma do anexo a esta Portaria Normativa.

Art. 2º Esta Portaria Normativa entra em vigor na data de sua publicação.

Art. 3º Revoga-se a Portaria Normativa nº 1.292/MD, de 26 de maio de 2014.

ALDO REBELO

(Publicado no D.O.U. nº 207 de 29 de outubro de 2015.)

REGISTRO DE MODIFICAÇÕES

NÚMERO DE ORDEM	ATO DE APROVAÇÃO	PÁGINAS AFETADAS	DATA	RUBRICA DO RESPONSÁVEL

SUMÁRIO

CAPÍTULO I - INTRODUÇÃO 13

1.1 Finalidade 13
1.2 Referências 13
1.3 Aplicação 13

CAPITULO II - CONCEITOS E DEFINIÇÕES 15

2.1 Ameaça 15
2.2 Ativo 15
2.3 Ativo de informação 15
2.4 Atributos de Segurança da Informação e das Comunicações 15
2.5 Auditoria 15
2.6 Centro de processamento de dados 15
2.7 Componentes Críticos do Sistema 15
2.8 Comunicação de dados 16
2.9 Controles de Segurança da Informação 16
2.10 Cultura e Organização de Segurança da Informação 16
2.11 Dado 16
2.12 Equipe de Tratamento de Incidentes de Rede (ETIR) 16
2.13 Evento de segurança da informação 16
2.14 Gestão de risco 16
2.15 Gestor de Segurança da Informação e das Comunicações (SIC) do SISMC² 16
2.16 Impacto 17
2.17 Incidente 17
2.18 Informação 17
2.19 Mentalidade se Segurança 17
2.20 Plano de Continuidade do Negócio 17
2.21 Quebra de Segurança 17
2.22 Risco 17
2.23 Segurança da Informação e das Comunicações (SIC) no SISMC² 17
2.24 Serviços de redes de telecomunicações 17
2.25 Serviços de TI 18
2.26 Serviços de TI próprios 18
2.27 Sistema de informação 18
2.28 Vistoria de Segurança da Informação (VSI) 18
2.29 Vulnerabilidade 18

CAPÍTULO III - ESCOPO 19

3.1 Abrangência 19
3.2 Objetivos 19
3.3 Atribuições 19
3.4 Informações 20
3.5 Regulamentação 21

CAPÍTULO IV - DIRETRIZES GERAIS 23

4.1 Tratamento da Informação 23
4.2 Gestão de Risco 24
4.3 Gestão de Continuidade do Negócio 24
4.4 Correio eletrônico 24

LISTA DE DISTRIBUIÇÃO

INTERNA	
ÓRGÃOS	**EXEMPLARES**
GABINETE DO MINISTRO DE ESTADO DA DEFESA	1
GABINETE ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS	1
CHEFIA DE OPERAÇÕES CONJUNTAS	1
CHEFIA DE ASSUNTOS ESTRATÉGICOS	1
CHEFIA DE LOGÍSTICA	1
ASSESSORIA DE DOUTRINA E LEGISLAÇÃO - **Exemplar Mestre**	1
SECRETARIA DE ORGANIZAÇÃO INSTITUCIONAL	1
SECRETARIA DE PESSOAL, ENSINO, SAÚDE E DESPORTO	1
SECRETARIA DE PRODUTOS DE DEFESA	1
CENTRO GESTOR E OPERACIONAL DOS SISTEMAS DE PROTEÇÃO DA AMAZÔNIA	1
PROTOCOLO GERAL	1
ESCOLA SUPERIOR DE GUERRA	1
HOSPITAL DAS FORÇAS ARMADAS	1
SUBTOTAL	**13**

EXTERNA	
ÓRGÃOS	**EXEMPLARES**
COMANDO DA MARINHA	1
COMANDO DO EXÉRCITO	1
COMANDO DA AERONÁUTICA	1
ESTADO-MAIOR DA ARMADA	1
ESTADO-MAIOR DO EXÉRCITO	1
ESTADO-MAIOR DA AERONÁUTICA	1
COMANDO DE OPERAÇÕES NAVAIS	1
COMANDO DE DESENVOLVIMENTO DOUTRINÁRIO DO CORPO DE FUZILEIROS NAVAIS	1
COMANDO DE OPERAÇÕES TERRESTRES	1
COMANDO-GERAL DE OPERAÇÕES AÉREAS	1
SUBTOTAL	**10**
TOTAL	**23**

CAPÍTULO I

INTRODUÇÃO

1.1 Finalidade

Prover diretrizes estratégicas para aperfeiçoar a gestão da Segurança da Informação e das Comunicações (SIC) no âmbito do Sistema Militar de Comando e Controle (SISMC²).

1.2 Referências

Os documentos consultados para a elaboração desta Política foram:

a) Decreto nº 3.505, de 13 junho de 2000 (institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal);

b) Portaria Normativa nº 2.091/MD, de 12 de julho de 2013 (dispõe sobre a Política para o Sistema Militar de Comando e Controle - MD31-P-01 - 2ª Edição/2012);

c) Instrução Normativa nº 01/EMCFA/MD, de 25 de julho de 2011 (aprova as instruções para a confecção de publicações padronizadas do Estado-Maior Conjunto das Forças Armadas - MD20-I-01 - 1ª Edição/2011);

d) Norma Técnica ABNT NBR ISO/IEC 27002:2013, de 8 de novembro de 2013 (Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação);

e) Norma Técnica ABNT NBR ISO/IEC 27001:2013, de 8 de novembro de 2013 (Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos);

f) Norma Complementar nº 03/IN01/DSIC/GSIPR, de 30 de junho de 2009 (diretrizes para elaboração de Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal);

g) Lei nº 12.527, de 18 de novembro de 2011 (regula o acesso a informações previsto na Constituição Federal e dá outras providências);

h) Decreto nº 7.724, de 16 de maio de 2012 (regulamenta a Lei nº 12.527, de 18 de novembro de 2011);

i) Decreto nº 8.135, de 4 de novembro de 2013 (dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional); e

j) Portaria Interministerial nº 141, de 2 de maio de 2014, dos Ministérios do Planejamento, Orçamento e Gestão (MPOG), das Comunicações (MC) e da Defesa (MD) (dispõe sobre as comunicações de dados da Administração Pública Federal direta, autárquica e fundacional).

1.3 Aplicação

Esta Política se aplica ao pessoal, à estrutura organizacional e à infraestrutura tecnológica do SISMC².

CAPÍTULO II

CONCEITOS E DEFINIÇÕES

2.1 Ameaça

Fator que possa causar algum incidente.

2.2 Ativo

Qualquer bem, tangível ou intangível, que tenha valor para a organização.

2.3 Ativo de informação

Meios de armazenamento, transmissão e processamento, sistema de informação, bem como local onde se encontram esses meios e as pessoas que a eles têm acesso.

2.4 Atributos de Segurança da Informação e das Comunicações

Os atributos clássicos de SIC, que também se aplicam ao SISMC², são os seguintes:

a) **confidencialidade**: propriedade de negar a disponibilização ou revelação da informação a indivíduos, entidades ou processos não autorizados nem credenciados;

b) **integridade**: propriedade de salvaguarda da exatidão e totalidade da informação, de forma a garantir que o conteúdo original da informação não seja modificado indevidamente por elemento humano ou qualquer outro processo;

c) **disponibilidade**: propriedade de assegurar que a informação esteja acessível e utilizável sob demanda de uma entidade autorizada;

d) **autenticidade**: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

e) **não-repúdio (irretratabilidade)**: propriedade de assegurar que, num processo de envio e recebimento de informações, nenhum participante originador nem destinatário de informação possa, em um momento posterior, negar a respectiva atuação.

2.5 Auditoria

Processos e procedimentos sistemáticos de levantamento de evidências que tem como objetivo verificar se os serviços de redes de telecomunicações e de tecnologia da informação atendem aos requisitos previamente especificados, em termo de referência ou projeto básico, para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações.

2.6 Centro de processamento de dados

Ambiente que concentra e gerencia recursos computacionais para armazenamento e tratamento sistemático de dados.

2.7 Componentes Críticos do Sistema

São recursos ou equipamentos vitais do sistema para os riscos envolvidos.

2.8 Comunicação de dados

É a transmissão, emissão ou recepção de dados ou informações de qualquer natureza por meios confinados, radiofrequência ou qualquer outro processo eletrônico ou eletromagnético ou ótico.

2.9 Controles de Segurança da Informação

São instrumentos utilizados para mitigar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser:

a) de natureza administrativa e técnica;

b) de gestão ou legal.

2.10 Cultura Organizacional de Segurança da Informação

Predisposição coletiva, no âmbito de uma organização, favorável à adoção de procedimentos de segurança da informação, cuja consecução se dá por intermédio de um processo gradativo que abrange a sensibilização, a conscientização, a capacitação e a especialização de segmentos específicos de seus recursos humanos.

2.11 Dado

Qualquer elemento definido em sua forma bruta, que, tomado isoladamente, não conduz, por si só, à compreensão de determinado fato ou determinada situação.

2.12 Equipe de Tratamento de Incidentes de Rede (ETIR)

É o grupo de militares e servidores, designados pelo Subchefe de Comando e Controle da Chefia de Operações Conjuntas do Estado-Maior Conjunto das Forças Armadas (CHOC/EMCFA), com a responsabilidade de, quando necessário, receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança da informação do $SISMC^2$.

2.13 Evento de Segurança da Informação

Ocorrência identificada de um sistema, um serviço ou uma rede, que indica uma possível violação da política de segurança da informação ou falha de controles ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

2.14 Gestão de risco

Conjunto de processos que permite identificar e implementar as medidas de proteção necessárias ao tratamento dos riscos aos quais estão sujeitos os ativos de informação, buscando equilibrá-los com os custos operacionais e financeiros envolvidos.

2.15 Gestor de Segurança da Informação e das Comunicações do $SISMC^2$

É o oficial ou servidor assemelhado, designado pelo Subchefe de Comando e Controle, responsável pela coordenação das ações de SIC no âmbito do $SISMC^2$.

2.16 Impacto

É o dano causado por um incidente.

2.17 Incidente

É um evento ou uma série de eventos de segurança da informação que tenham probabilidade de comprometer quaisquer dos atributos de SIC.

2.18 Informação

Dados organizados e inseridos em um contexto, de maneira a propiciar elementos de análise a seu usuário, permitindo a tomada de decisões.

2.19 Mentalidade de Segurança

Predisposição individual favorável à adoção de procedimentos de segurança da informação, cuja consecução se dá por intermédio de um processo constituído de duas etapas: sensibilização e conscientização.

2.20 Plano de Continuidade do Negócio

Descreve as informações necessárias e as medidas a serem tomadas por uma instituição para evitar a interrupção de suas operações ou, caso ocorram, que seus processos voltem o mais rápido possível à plena operação ou a um estado mínimo aceitável.

2.21 Quebra de segurança

Ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações.

2.22 Risco

Qualificação da insegurança, por meio da combinação de probabilidade, com a gravidade de ocorrência de um evento.

2.23 Segurança da Informação e das Comunicações no SISMC²

É o conjunto de ações que objetivam viabilizar e assegurar a proteção das informações e dos ativos de informação do SISMC², de modo a permitir a utilização eficaz e eficiente de seus serviços somente a usuários autorizados, bem como impedir a intrusão e a modificação desautorizada de dados ou informações armazenados, em processamento ou em trânsito.

2.24 Serviços de redes de telecomunicações

Provimento de serviços de telecomunicações, de tecnologia da informação, de valor adicionado e de infraestrutura para redes de comunicação de dados.

2.25 Serviços de TI

Provimento de serviços de desenvolvimento, implantação, manutenção, armazenamento e recuperação de dados e operação de sistemas de informação, projeto de infraestrutura de redes de comunicação de dados, modelagem de processos e assessoramento técnico, necessários à gestão da segurança da informação e comunicações.

2.26 Serviços de TI próprios

Conjunto de serviços de tecnologia da informação prestados por meio de plataformas desenvolvidas pelo próprio órgão ou entidade, cuja posse, gestão, administração e responsabilidade pela operação sejam exclusivas do próprio órgão ou entidade da Administração Pública Federal.

2.27 Sistema de informação

Conjunto de componentes inter-relacionados que coleta, processa, armazena e distribui informação para dar suporte à tomada de decisão e ao controle de uma organização. Tais componentes podem envolver *software*, meios de comunicações, computadores, redes de computadores, dados e informações, especificações e procedimentos para operação, uso e manutenção.

2.28 Vistoria de Segurança da Informação (VSI)

Procedimento de avaliação periódica dos processos das atividades, dos controles de segurança da informação e dos sistemas que trafegam, processam ou armazenam informações, conduzido preferencialmente de forma independente da organização militar vistoriada, com o objetivo de verificar a sua efetividade e conformidade com as políticas, diretrizes, doutrinas e normas de SIC vigentes. O resultado das VSI pode indicar a necessidade de realização de auditoria em ativos de rede ou sistemas que atendem ao SISMC².

2.29 Vulnerabilidade

Conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação e comunicações.

CAPÍTULO III

ESCOPO

3.1 Abrangência

Esta Política se aplica a todos os componentes dos sistemas de informação do SISMC², para o conhecimento, o planejamento, o preparo e a execução de ações de SIC.

As informações que tramitam pelo SISMC², sob custódia do EMCFA e dos demais órgãos integrantes, exigem regulamentação específica para a sua proteção, uma vez que constituem recursos essenciais para o funcionamento da Estrutura Militar de Defesa (EttaMiD), devendo ser protegidas e preservadas, por meio de atividades de SIC. A regulamentação da SIC compreende um conjunto de diretrizes e normas a serem seguidos por todos os componentes do SISMC², em conformidade com os propósitos estabelecidos neste documento.

3.2 Objetivos

Esta Política possui os seguintes objetivos:

3.2.1 Promover a uniformidade conceitual e doutrinária, orientando os órgãos responsáveis por sistemas de informação do SISMC² na elaboração de instrumentos normativos que os capacitem a assegurar que as informações que por ele transitem ou nele estejam armazenadas ou sejam processadas contenham os atributos de segurança da informação;

3.2.2 Promover a interoperabilidade das soluções de SIC no âmbito do SISMC²;

3.2.3 Promover a capacitação de pessoal para o desenvolvimento de competência científico-tecnológica em segurança da informação, no EMCFA e nas Forças Armadas, visando viabilizar a formação de cultura organizacional de segurança da informação.

3.3 Atribuições

3.3.1 Cabe ao Subchefe de Comando e Controle da CHOC/EMCFA:

a) definir a estrutura de gestão de SIC;
b) acompanhar e coordenar as atividades de gestão de SIC no âmbito do SISMC²;
c) propor grupos de trabalho para tratar de temas e propor soluções específicas sobre SIC;
d) propor, analisar e aprovar normas relativas à SIC, em conformidade com as legislações vigentes sobre o tema;
e) nomear o Gestor de SIC do SISMC² e a ETIR.

3.3.2 Cabe ao Gestor de SIC do SISMC²:

a) promover cultura de SIC no âmbito do SISMC², por intermédio de atividades de sensibilização, conscientização, capacitação e especialização;

b) acompanhar as investigações e as avaliações dos danos decorrentes de incidentes porventura ocorridos;
c) propor recursos necessários às ações de SIC;
d) coordenar a ETIR;
e) promover e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SIC no âmbito do SISMC²;
f) manter contato permanente e estreito com o Gestor de Segurança da Informação e Comunicações da administração central do Ministério da Defesa (GSIC-ACMD) e com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSI-PR) para o trato de assuntos relativos à SIC;
g) propor normas e procedimentos relativos à SIC no âmbito do SISMC², em conformidade com as legislações existentes sobre o tema;
h) assessorar o Subchefe de Comando e Controle na implementação das ações de SIC no âmbito do SISMC².

3.3.3 Cabe à ETIR:

a) tratar os incidentes de rede em estrito cumprimento às normas em vigor;
b) assessorar o Gestor de SIC no trato de assuntos relativos a incidentes de rede;
c) participar de grupos de trabalho, coordenados pelo Gestor de SIC, relativos ao tratamento de incidentes de rede;
d) ligar-se com equipes congêneres na ACMD, nas Forças Armadas e no GSI-PR, mantendo permanente canal técnico para compartilhamento de informações e coordenação de ações relativas ao tratamento de incidentes de rede.

3.3.4 Cabe aos órgãos integrantes do SISMC², nos seus respectivos âmbitos de atuação:

a) buscar incessantemente a redução da dependência externa em relação a sistemas, equipamentos e dispositivos relacionados à SIC;
b) estabelecer normas necessárias à efetiva implementação da SIC;
c) promover as ações necessárias à implementação e manutenção da SIC;
d) compartilhar as informações sobre a ocorrência de incidentes que violem os requisitos de segurança e as medidas adotadas para saná-los;
e) submeter à Subchefia de Comando e Controle as propostas de alterações desta Política.

3.3.5 Cabe aos usuários do SISMC²:

a) observar a presente Política e cumprir todas as normas e os procedimentos de SIC vigentes;
b) tratar a informação como um ativo a ser protegido no contexto da Segurança/Defesa Nacional.

3.4 Informações

As informações que tramitam pelo SISMC², sob custódia do EMCFA e dos outros órgãos integrantes, exigem regulamentação específica para sua proteção, uma vez que constituem recurso essencial para o funcionamento da EttaMiD, devendo ser protegidas e preservadas, por meio de atividades de SIC.

3.5 Regulamentação

A regulamentação da SIC compreende um conjunto de diretrizes e normas emitidas pelo EMCFA, em conformidade com os objetivos estabelecidos nesta Política. O cumprimento das diretrizes e normas de SIC é de responsabilidade de todos os componentes, permanentes ou eventuais, do SISMC².

A documentação normativa de órgão integrante, permanente ou temporário, do SISMC² sobre SIC deve considerar esta Política como referência básica para a sua elaboração.

CAPÍTULO IV

DIRETRIZES GERAIS

4.1 Tratamento da Informação

A informação é um ativo e, dessa forma, deve ser adequadamente manuseada e protegida.

A informação transita, é armazenada ou processada sob diversas formas, tais como: sistemas de informação, diretórios de rede, bancos de dados, mídia impressa, magnética ou ótica, dispositivos eletrônicos, equipamentos portáteis, microfilmes e até mesmo por meio da comunicação oral.

O armazenamento, a recuperação e o processamento de informações devem ser realizados em **centros de processamento de dados** de órgãos integrantes do SISMC².

Toda a informação de interesse deve ser classificada e tratada de acordo com seu grau de sigilo, valor, requisitos legais, sensibilidade e criticidade, bem como utilizada unicamente para a finalidade para a qual foi autorizada. As informações devem, sobretudo, ser protegidas de riscos e ameaças. Nesse contexto, a informação é um ativo e deve ser adequadamente manuseada e protegida. Considera-se necessário o emprego de sistemas de Tecnologia da Informação e Comunicações (TIC) nas atividades de Comando e Controle (C²) das operações militares (conceito de **Command, Control, Communications, Computers, and Intelligence** - C4I), com os adequados atributos de SIC, para a consecução rápida, precisa e oportuna do ciclo de C² necessário para obtenção de vantagens decisivas, frente à crescente complexidade das crises e dos conflitos modernos.

As comunicações de dados no SISMC² serão estruturadas e efetuadas em conformidade com as seguintes diretrizes:

I - criação, desenvolvimento e manutenção de ações de segurança da informação e comunicações;

II - planejamento, articulação e gestão integrada das políticas de segurança da informação e comunicações;

III - redução de pontos de vulnerabilidade por meio da padronização, integração e interoperabilidade das redes de telecomunicações e dos serviços de tecnologia da informação contratados; e

IV - implementação de ações e procedimentos que assegurem a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, incluindo a adoção de programas e equipamentos que possam ser auditados.

4.1.1 Rede de Dados

O emprego de sistemas de TIC nas atividades de C² pressupõe o uso de computadores em rede. Para garantir informações protegidas de riscos e ameaças, impõe-se a necessidade de emprego de redes próprias no âmbito do SISMC², com ativos próprios e adequados ao uso operacional militar da informação e aos atributos de SIC previstos nesta Política.

4.1.2 Centro de Processamento de dados

O tratamento adequado da informação no âmbito operacional militar, empregando sistemas de TIC, impõe a necessidade de que o armazenamento, a recuperação e o processamento de dados sejam realizados em Centros de Processamento de Dados (CPD) instalados em órgãos integrantes do SISMC² adequados ao uso operacional militar

da informação e aos atributos de SIC previstos nesta Política e capazes de prover os serviços de TI próprios.

4.1.3 Comunicação de Dados Operacionais Militares

As comunicações de dados militares operacionais no âmbito do SISMC² serão realizadas de acordo com doutrina própria, por meio de Sistemas de TIC adequados às necessidades operacionais das Forças Armadas, devidamente definidas pelo EMCFA e considerando os aspectos de SIC previstos nesta Política. Estabelece-se como diretrizes básicas:

I - redução de pontos de vulnerabilidade, por meio da padronização, integração e interoperabilidade das redes de telecomunicações e dos serviços de TIC; e

II - implementação de ações e procedimentos que assegurem a disponibilidade, a integridades, a confidencialidade e a autenticidade das informações.

4.1.3.1 As comunicações de dados de cunho eminentemente administrativo no âmbito das Forças Armadas deverão ser realizadas em conformidade com os dispositivos previstos no item 1.2, alíneas “i” e “j”.

4.2 Gestão de Risco

A gestão de risco dos ativos de informação deve constituir processo contínuo, em conformidade com o arcabouço normativo vigente no SISMC² e legal vigente. Deve também visar à proteção do SISMC² por intermédio do tratamento dos riscos, conforme sua viabilidade.

4.3 Gestão de Continuidade do Negócio

Os ativos de informação devem ser protegidos contra problemas decorrentes de defeitos, desastres, indisponibilidades e falhas, por intermédio de elaboração e execução de Planos de Continuidade, dentre outras atividades de gestão, visando à instrução e à manutenção da capacitação dos integrantes do SISMC².

4.4 Correio eletrônico

O serviço de correio eletrônico é oferecido como um recurso profissional para apoiar os usuários do SISMC², no cumprimento dos objetivos institucionais, sendo passível de auditoria e fiscalização.

É vedada a utilização de serviços de correio eletrônico e suas funcionalidades complementares que não sejam disponibilizados pelos órgãos integrantes do SISMC².

4.5 Acesso à Internet

O acesso à internet deve ser permitido somente para pesquisas na rede que contribuam no desenvolvimento do trabalho sendo executado, para publicação de serviços externos, onde o uso de rede compartimentada for inviável, para emprego de redes privativas virtuais (*Virtual Private Networks* - VPN) e videoconferências com interlocutores que não façam parte do SISMC², mediante adoção de controles de segurança da informação adequados. Não é permitido ao acesso a redes sociais e de mensagens instantâneas por provedores que não sejam integrantes do SISMC².

4.6 Restrição e controle de acesso

Todos os usuários das informações do SISMC^2 devem ter acesso liberado somente aos recursos necessários e indispensáveis ao desempenho de suas atividades.

Todo usuário deve ter uma identificação única, pessoal e intransferível, qualificando-o, inequivocamente, como responsável por qualquer atividade desenvolvida sob sua identificação.

Devem ser instituídas normas que estabeleçam procedimentos, processos e mecanismos que assegurem o controle de acesso às instalações, às informações e aos sistemas de informação.

4.7 Auditoria e Conformidade

Auditorias devem ser realizadas, no mínimo, anualmente, para verificar a conformidade e a efetividade dos controles de SIC implantados no SISMC^2.

Todos os usuários estão sujeitos à auditoria e fiscalização ao utilizar os recursos do SISMC^2.

4.8 Penalidades

O descumprimento ou a violação desta Política de Segurança da Informação e Comunicações e demais normas e procedimentos estabelecidos relativos a ela terá implicação administrativa, civil e penal, segundo as normas e a legislação vigentes, de acordo com a gravidade do ato praticado.

4.9 Auditorias de Sistemas de TIC

Deve-se buscar, no âmbito do SISMC^2, que os Sistemas de TIC e os serviços de TI operacionais militares sejam auditáveis, de forma a reduzir riscos à SIC. Nesse sentido, e considerando as restrições operacionais que seriam impostas às Forças Armadas pela negação do emprego de sistemas e serviços de TIC que não possuam características de auditabilidade, devem ser tomados cuidados especiais na implementação e utilização dos respectivos produtos adquiridos ou desenvolvidos para o SISMC^2, de forma a garantir atributos de SIC adequados.

CAPÍTULO V

DISPOSIÇÕES FINAIS

5.1 Atualização

Esta Política e seus instrumentos normativos derivados deverão ser revisados sempre que se fizer necessário, com apoio de representantes dos setores especializados de Tecnologia da Informação e Comunicações das três Forças Armadas, não excedendo o período máximo de três anos de sua promulgação.

5.2 Aprimoramento

Com a finalidade de aprimorar esta Política, solicita-se que as sugestões de modificações sejam enviadas ao EMCFA, no seguinte endereço:

MINISTÉRIO DA DEFESA
Estado-Maior Conjunto das Forças Armadas
Assessoria de Doutrina e Legislação
Esplanada dos Ministérios - Bloco Q - 5º Andar
Brasília - DF
CEP - 70049-900
adl1.emcfa@defesa.gov.br

Ministério da Defesa
Estado-Maior Conjunto das Forças Armadas
Brasília, 29 de outubro de 2015